UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	15 Cr. 333, 19 Cr. 658 (LTS)
ANDREI TYURIN, a/k/a "Andrei Tiurin,"	:	
Defendant.	:	

GOVERNMENT'S SENTENCING MEMORANDUM

AUDREY STRAUSS
Acting United States Attorney for the
Southern District of New York

Eun Young Choi
Assistant United States Attorney
- Of Counsel -

TABLE OF CONTENTS

I. PRELIMINARY STATEMENT

The United States respectfully submits this memorandum in connection with the sentencing of defendant Andrei Tyurin, scheduled for November 17, 2020 at 9:00 AM, and in response to defendant's sentencing memorandum filed on November 4, 2020 ("Mem.").

Tyurin is a brazen and prolific computer hacker responsible for executing a massive computer hacking campaign. From approximately 2007 until 2015, Tyurin, working with his partner and co-conspirator Gery Shalon, infiltrated the networks of over a dozen companies, including U.S. financial institutions, brokerage firms, financial news publishers, and other U.S. companies. As part of his international campaign, Tyurin's hacks included one of the largest thefts of customer data from a U.S. financial institution in history (J.P. Morgan Chase, referred to as "Victim-1" in the Indictment)—over 80 million individuals for that theft alone—and inflicted millions of dollars in damage to the victims which he hacked. For his efforts, which included not only hacking into the victim companies' networks, but also maintaining persistent access to the victims' systems so that data could be regularly and routinely stolen from these companies, Tyurin was paid over $19 million. And when it became apparent that his unauthorized access into Victim-1 had been detected by the company and that law enforcement was on the case, Tyurin and Shalon worked in tandem to destroy evidence of their crimes: the online infrastructure Tyurin used in furtherance of the attacks, which could identify him and Shalon as the individuals responsible.

Tyurin executed his crimes deliberately and over an extended period of time, and did so primarily for his own self-enrichment. Using his specialized technical skills, Tyurin was able to infiltrate and steal from some of the world's most sophisticated financial institutions based in the United States, profiting from his thefts while working in anonymity thousands of miles

away in Russia. And despite Tyurin and his co-defendant Shalon's best efforts to destroy the digital trail linking them to these hacks, U.S. law enforcement not only successfully identified Tyurin but brought him to justice before this Court—a difficult achievement in the world of international cybercriminal investigations and prosecutions. This outcome was only possible through a significant and coordinated effort by U.S. authorities, working alongside their international counterparts in numerous different countries. Consequently, Tyurin's sentence should reflect not only the enormous destructive impact that he has inflicted through his criminal hacking, but also serve as a clear message to deter other would-be criminals, here and elsewhere, from hacking and victimizing U.S. companies and their customers.

A Guidelines term of imprisonment is warranted to reflect the seriousness of the offense, to promote respect for the law, to avoid unwanted sentencing disparities, and perhaps most importantly, to provide for adequate deterrence for a case of this magnitude.

II. STATEMENT OF FACTS

A. The Defendant's Offense Conduct

Until his arrest in July 2015, Gery Shalon, an Israeli, Georgian, and Russian citizen based in Tel Aviv, was the leader of a sprawling cybercriminal empire, which included Andrei Tyurin and his co-conspirators Joshua Samuel Aaron and Ziv Orenstein. Shalon and his co-conspirators ran a variety of criminal business, including online gambling and pharmaceutical companies which catered to U.S. customers, an illicit payment processing operation that processed credit and debit card transactions for a variety of criminal activities for themselves and others (including their own gambling and online pharmaceuticals transactions, as well as other "high risk" lines of business), and an unlicensed Florida-based bitcoin company by the

name of Coin.mx.[1] The key to Shalon's success in each of these lines of criminal activity was the defendant, known to Shalon only as "Andrei." Tyurin's hacking activities played a crucial role in Shalon's criminal conglomerate, allowing Shalon to maintain a competitive edge in his operation of his diversified and lucrative criminal schemes. (*See* Presentence Report ("PSR") ¶ 31).

Specifically, in furtherance of Shalon's various criminal activities, Tyurin hacked companies, including companies located in the United States, for the purpose of obtaining customer data or procuring information that could be used to give Shalon a competitive advantage, such as internal information from competitors or financial auditors who might detect Shalon's criminal activities. This hacking activity included Tyurin's successful infiltration of major U.S. financial institutions and financial sector businesses (including but not limited to J.P. Morgan Chase Bank, E*Trade, Scottrade, and the Wall Street Journal), in an effort to steal customer lists in furtherance of a securities pump-and-dump scheme orchestrated by Shalon and Aaron. In order to facilitate Tyurin's hacking activity, Shalon and his co-conspirators procured computer network infrastructure, including computer servers located in Egypt, the Czech Republic, South Africa, Brazil, and elsewhere. Tyurin then used this infrastructure, from his home in Moscow, to gain unlawful access to the companies' computer networks and to receive data stolen from those networks as a result of his work. Tyurin would maintain persistent access over extended periods of time to the victims' networks, and would regularly refresh the stolen data by repeatedly downloading information from these companies, so that Shalon's

[1] As is described further below, the U.S.-based individuals who operated or were affiliated with Coin.mx were separately charged and sentenced in the case *United States v. Murgio*, 15 Cr. 769 (AJN).

conglomerate could stay one step ahead in their knowledge of their competitors' activities and the efforts of the victim companies to detect their criminal activity, and to ensure that their lists of customer data were as up-to-date as possible. (*See* PSR ¶¶ 32-33).

Electronic communications between Shalon and Tyurin seized at the time of Shalon's arrest establish that they were in continuous contact with one another regarding their criminal efforts. As a general matter, Shalon would provide Tyurin which victim companies to target for computer intrusion, and indicate the type of data he sought to steal from the victim company, and the purpose of the use of the data that Tyurin was stealing. Tyurin, in turn, would provide Shalon with updates as to the status of his efforts, whether and when he was able to locate the data that Shalon had instructed him to steal, the size of the data that Tyurin was able to take from the victim companies, Tyurin's efforts to transmit that stolen data to Shalon, and whether Tyurin was able to maintain persistent access to victim companies' networks and databases over extended periods of time. In certain instances when Shalon and his co-conspirators lost access to certain networks for which Tyurin had set up persistent access, Shalon would ask Tyurin to go back into the company's networks again, so that Shalon and his co-conspirators could continue to access the victim company's data. Their activities came to an end in July 2015, upon Shalon's arrest at his home in Israel. It was through the careful combing of the contents of Shalon's computers and digital devices, seized by Israeli authorities at the time of Shalon's arrest, that U.S. law enforcement was able to find details regarding "Andrei," including references to his travel and financial transactions made by Shalon to send "Andrei" proceeds of their joint criminal enterprise. Through these efforts, U.S. law enforcement was able to determine "Andrei's" true identity, leading to his arrest and successful extradition from Tbilisi, Georgia. (*See* PSR ¶ 33).

As is described in further detail below, each of Shalon's criminal schemes depended entirely on data stolen by Tyurin to succeed. And as the scope of Shalon's criminal businesses grew, so did the number and types of victims that Tyurin targeted, starting with companies known to be used for email marketing, and then proceeding to online casinos, a merchant risk intelligence firm which detects payment processing fraud, and then finally the hacks of companies in the U.S. financial sector.

1. Online Casinos

From approximately 2007 through his arrest in July 2015, Shalon owned and operated multiple unlawful internet casinos that accepted online bets from U.S.-based customers in violation of United States law. In order to grow his online casino business, Shalon sought the assistance of hackers on criminal online forums. It was on one of these forums that, in 2007, Shalon met Tyurin, an established hacker who offered to sell to Shalon approximately 50,000 email addresses for use to market his online casinos. When this initial trove of stolen data yielded a substantial increase of casino business for Shalon, Tyurin's talents were proven to be valuable to Shalon. And although initially Tyurin's hacking skills were sought for use by many different criminals on these forums, over time, Tyurin chose to work exclusively for Shalon, because Tyurin understood his opportunity for financial gain was greatest with Shalon. It was from this mutually beneficial financial arrangement that Tyurin and Shalon's long-lasting criminal partnership was formed.

Tyurin applied his hacking skills in multiple different ways to promote and grow Shalon's online casino business. Tyurin first provided Shalon with lists of potential customers for the purpose of online targeted marketing. Tyurin had procured these lists by hacking major companies, including U.S.-based companies that provided email marketing services for other

businesses, and stealing their data. But a more efficient and effective mechanism to grow the casino business emerged: hacking other internet gambling businesses, including Shalon's competitors, as well as an internet gambling software company. By doing so, Tyurin could not only steal customer information for individuals who wished to gamble online to provide to Shalon, but Tyurin could also provide Shalon with insight as to how the victim casino companies' networks were organized, and to secretly read the emails of the victim companies' executives to stay one step ahead of the competition. (*See* PSR ¶ 41).

As a result of Tyurin's efforts, the total volume of Shalon's casino business grew, as did its profits. From approximately January 2008 to June 2015, the volume of deposits made into Shalon's online casinos was $438,711,306, including $386,065,949 in illegal casino volume from U.S. customers. During the same period, Shalon's online casinos received approximately $80,112,953 in illegal profits.

2. Illegal Payment Processing

From approximately 2011 through his arrest in July 2015, in order to ensure that his various criminal enterprises were able to process credit and debit card payments made by their customers for Shalon's various criminal lines of business, Shalon ran a sophisticated illegal multinational payment processing system. (*See* PSR ¶ 43).

By means of background, major credit card networks, such as MasterCard and Visa, operate systems whereby merchants are categorized according to a merchant category code ("MCC"), which helps identify the type of business of the merchant. Certain MCC codes represent illicit or otherwise "high risk" business, including codes for transactions involving online gambling, online pharmaceuticals, and money services businesses such as bitcoin exchanges. Thus, to allow for online deposits by customers of Shalon's internet casinos and

his bitcoin exchange, as well as for payments for purchases on Shalon's online pharmacies and other illicit transactions, Shalon and his co-conspirators deliberately misidentified and miscoded these transactions, in order to trick banks into processing otherwise banned transactions. For example, through their payment processing scheme, Shalon, Orenstein, and their co-conspirators arranged for money received from U.S. gamblers to be disguised as payments to phony online non-gambling merchants, such as wedding dress and pet supply stores, in order to trick U.S. and other financial institutions into allowing the transactions to be completed. Through his illicit payment processing program, predicated on miscoding, Shalon and his co-conspirators fraudulently processed hundreds of millions of dollars' worth of transactions. (*See* PSR ¶ 44).

Maintaining the online payment processing infrastructure was crucial to each of Shalon's criminal lines of business. However, banks and the credit card networks became better at detecting fraudulent and criminal online payments, and then shutting down the merchant accounts used to process these transactions. The growing fines levied against Shalon's accounts, as well as the number of instances in which accounts were being permanently shut down by banks, posed increasing challenges to the profitability of Shalon's criminal activities. Thus, Shalon instructed Tyurin to hack into [redacted] identified as "Victim-12" in the Indictment, a merchant risk intelligence firm based in Bellevue, Washington, which assessed merchant risk and compliance for credit card issuers and others, including by detecting merchants that accepted credit card payments for unlawful goods or services. Victim-12 conducted such monitoring in part by maintaining credit card numbers that it would then use to audit potentially criminal businesses online, by conducting credit card transactions with those businesses and monitoring the financial trail of the transactions, and thus

determine whether the online businesses were engaged in miscoding. Tyurin successfully was able to maintain persistent access of Victim-12's systems, and allow for Shalon and his co-conspirators to monitor Victim-12's fraud detection efforts, including by reading emails of Victim-12 employees, so they could take steps to evade detection by Victim-12 of their unlawful payment processing scheme. In addition, Tyurin would download lists of credit and debit card numbers Victim-12 employees were using to make undercover purchases of illicit goods in the course of their efforts to audit and detect unlawful merchants. By collecting the credit and debit card numbers used by Victim-12, Shalon and his co-conspirators were able to undermine Victim-12's auditing function by implementing countermeasures against Victim-12's efforts, including by blocking or automatically declining any transactions from those credit cards used by Victim-12 to detect fraudulent merchant accounts. (*See* PSR ¶ 45).

3. The Infiltration of Financial Sector Companies and Firms

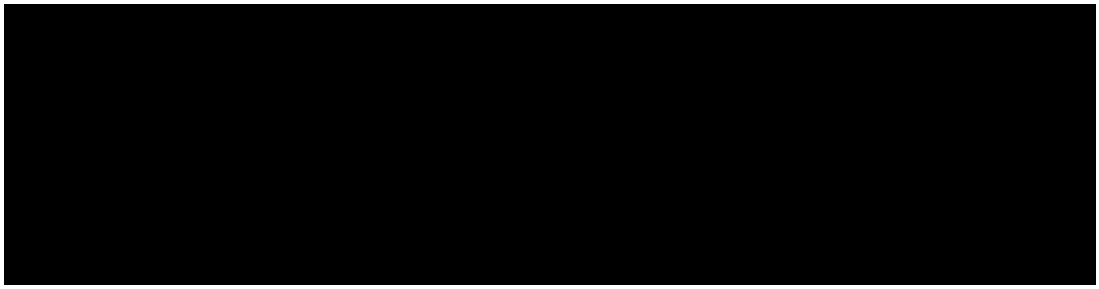
From approximately 2012 until 2015, Shalon, along with Joshua Samuel Aaron, and others, operated lucrative securities market manipulation schemes in the United States. Shalon, Aaron, and their co-conspirators would identify specific companies whose stock would be targeted for manipulation. In certain instances, those companies were already publicly traded, and in other instances, Shalon, Aaron, and their co-conspirators worked to cause those companies to become publicly traded, including by executing reverse mergers with publicly traded shell corporations in their control. Shalon and Aaron would then either agree upon a certain price, either in terms of dollars or shares of the targeted stock, for their role in promoting the targeted stock, or instead acquire control over all or substantially all of the free-trading shares of the targeted stock so as to benefit from the manipulation. Shalon and Aaron would artificially inflate the stock's price and trading volume, including through the dissemination of

materially misleading and unsolicited promotional materials, such as emails and hard copy mailers, that falsely touted the stock in order to trick others into buying it. After causing the stock's price and trading volume to increase artificially during the days or weeks of a deceptive promotional campaign for the stock, members of the conspiracy, including at times Shalon and Aaron, began selling their shares in a coordinated fashion, often resulting in millions of dollars in profits per stock to members of the conspiracy. (*See* PSR ¶ 36).

In order for the stock manipulation scheme to function, Shalon and Aaron needed lists of individuals to whom their fraudulent promotions would be directed. Accordingly, Shalon, Aaron, and Tyurin engaged in the hacks of U.S. financial sector firms and companies in part to acquire email and mailing addresses, phone numbers, and other contact information for potential victims to whom they could send such deceptive communications. Aaron would research various companies as targets to hack, and then open online accounts at the banks and companies that were to be targeted. Aaron would provide information relating to those online accounts (including but not limited to login credentials and header information for communications sent by the victim company to its customers who held online accounts) to Shalon, who in turn would instruct Tyurin which companies to hack, and pass the information for online accounts that was provided by Aaron so that Tyurin could perform network reconnaissance in furtherance of the hack, and identify where in the victim company's databases the relevant customer data was contained. Tyurin then worked to infiltrate the victim company's databases, which he would download and send to Shalon. Tyurin also worked to maintain persistent access to those victim companies' networks, such that Tyurin could refresh the customer data and download updated data for Shalon. Once downloaded, Shalon would provide the raw customer data to an employee, who in turn extracted the information that

Shalon sought and transposed it into a useable format at Shalon's direction. (*See* PSR ¶ 37).

In total, Tyurin stole customer data for over 100 million customers with regard to the financial sector hacks alone. These include the following estimates for certain of the victim companies in the financial sector hacks:



(*See* PSR ¶¶ 38-40).

4. Efforts to Evade and Obstruct Law Enforcement and the Destruction of Evidence

Once the hack into J.P. Morgan Chase had been detected and reported in the press, Shalon and Tyurin engaged in obstruction of the investigation, including the destruction of evidence in order to avoid their being identified as the individuals responsible for the intrusions. According to electronic communications seized from Shalon's devices, on August 16, 2014, Tyurin told Shalon that he noticed that his criminal activity might have been detected by J.P. Morgan Chase, because several of the IP addresses he was using to access the network had been banned. Tyurin noted it was not clear whether the hack had been detected, or instead if Chase had changed its passwords, but stated to Shalon "it's dangerous, if they detected they will probably be carefully monitoring for some time," but noted luckily he had already downloaded a significant portion of J.P. Morgan Chase's customer data by that point in time. On August 28, 2014, Shalon sent a link to Tyurin of an article from a Russian language news organization disclosing that J.P. Morgan Chase had been hacked, and that U.S. law enforcement was investigating the crime. Shalon wrote "I think we need to kill the servers" that they used to

steal the data. Tyurin agreed, and provided Shalon with the IP addresses for the specific servers that they had used. (PSR ¶ 46).

Tyurin then sent a link to a U.S. publication regarding the J.P. Morgan Chase hack and subsequent investigation, which contained more detail about the intrusion. Tyurin wrote to Shalon "We're caught" "I wasn't careful doing something" "Probably because of software on Windows," to which Shalon responded with an expletive, and "Forget it, we are killing the servers." Shalon then stated that he had talked to the company who hosted the servers at issue, and relayed to Tyurin that the hoster had asked Shalon what they should expect now that the hack was being investigated by the FBI, and that Shalon had instructed him to "physically throw the servers out." Tyurin responded "they will come and ask for discs" "And will ask who ordered the servers."

Later, Shalon told Tyurin that the hoster had received a court request to supply to them the contact information he had for Shalon. When the two discussed the risk that the hoster would provide the customer information for the servers they had rented that might risk identifying them, Tyurin suggested that they provide the hoster with false identity information, to in turn provide to the FBI:

Tyurin:	<in> We need to think of something\n[15:52:39] <in> Like we were resellers \n[15:52:48] <in> So if anything we can give this legend out.\n[15:53:00] <in> or that we were hacked[2]
Shalon:	Yes, but they will ask for contacts.
Shalon:	Even if [we] are resellers.
Shalon:	Well, you know, it's hard to believe that they are that smart.

[2] In this communication, Tyurin appears to be suggesting that they pose as "resellers" who rented the servers from the hoster in order to resell space on those servers to others (and thus were not the end users responsible for the hacking) or that they pose as victims of a hack, so they could maintain the fiction that the servers were used in the hacking of J.P. Morgan Chase without their knowledge.

```
Tyurin:    Yes, they aren't smart.
Tyurin:    They will try to look for all the leads.
Tyurin:    Maybe if something doesn't work out they will
           forget it.
Tyurin:    There are many problems if everything is in
           different countries.
Tyurin:    It's hard for them to look.
Shalon:    [Hoster]: Sorry was on call
           [Hoster]: For now do nothing - do not contact
           them. I will get more info from them.
           [Hoster]: They have given me a court request to
           supply your contact data we have.
Tyurin:    He is simply a prostitute in Poland.
Shalon:    Yes.
Shalon:    They are working very fast.
Tyurin:    Maybe we should give other person's data, not
           yours?
Tyurin:    To speak with them through a different name there?
Tyurin:    Like you are some Arab.
Shalon:    He wrote to me privately:
Shalon:    Hello,\n\nI need to supply some data as I am bound
           by law to supply the data if they request this
           through a court order.\n\nWhat are these
           people?\n\nI am obliged to give what they
           want.\n\nWhat do you suggest?
Tyurin:    Create a fake contact information for yourself
Tyurin:    And give it to him,
Tyurin:    Or buy from somebody.
```

When Shalon suggested that he pay the hoster $50,000 to help provide false identity information to the FBI, Tyurin suggested that Shalon make the payment in bitcoin "so that they don't nitpick the transaction"; that they provide the hoster with a Belarussian or Ukranian passport as the false identity; and that they pay the hoster some money upfront with "[t]he rest later, when everything is ok." Despite this, Tyurin took some comfort in the fact that "I think that what appeared in the news" regarding the hacking "was a leak" that happened "too fast," and that "[b]ecause of it they may not be able to have a good investigation" into the incident. As is reflected in the above-excerpted chats, Tyurin also understood the challenge for U.S. authorities in conducting this investigation in light of the online infrastructure being located in various international jurisdictions: "There are many problems if everything is in different

countries. It's hard for them to look."

At bottom, however Tyurin was concerned about the chances that he and Shalon would be identified: "Crap, if only America wasn't so serious, it would have been easier" "We didn't need to be scared that servers would be taken away." Shalon responded with his view regarding U.S. authorities: "They are very powerful." Tyurin, moreover, understood that because he was in Russia, the chances that he would be arrested were zero, noting to Shalon "I simply won't leave Russia" and "They won't get me here" "100% if I don't leave." Tyurin even attempted to convince Shalon to join him in Russia for some period of time. But, as law enforcement's efforts continued, the two spent hours discussing how to preserve their enterprise, including the following:

```
Tyurin:    Tell me if you need anything from me.
Shalon:    No, nothing.
Shalon:    It's important for me
Shalon:    That they don't get you.
Shalon:    Tell me what to do
Shalon:    And I will do it.
Shalon:    Sitting here.
Tyurin:    Don't think about me, even if I get a visit from
           police here they will only come to shake my
           hand.:)
Tyurin:    To shake.
Tyurin:    You are more important,
Tyurin:    And business.
Tyurin:    So that those bitches don't ruin anything.
```

5. Financial Gain to Tyurin

Shalon and Tyurin would expressly discuss transfers of money that Shalon would make to Tyurin as payment for his efforts, including through cash deliveries and transfers through a Russian-based money services business. The Government has conservatively estimated that Tyurin earned approximately $19,214,956 for his work for Shalon over the years. (PSR ¶ 47).

B. The Defendant's Arrest and Plea

Tyurin was arrested after traveling from Russia to Georgia on or about December 12, 2017. At the end of extradition proceedings, he was ordered extradited to the United States, where he was brought into U.S. custody on September 7, 2018.

On September 23, 2019, Tyurin pleaded guilty before the Court pursuant to a plea agreement to Counts One (conspiracy to commit computer hacking), Two (wire fraud), Eight (Unlawful Internet Gambling Enforcement Act conspiracy), and Nine (conspiracy to commit wire and bank fraud for unlawful payment processing) of the S4 Indictment in 15 Cr. 333; and Counts One (wire fraud conspiracy) and Five (computer fraud and identity fraud conspiracy) of the Indictment in 19 Cr. 658, which constituted the charges brought in the Northern District of Georgia.

III. THE GUIDELINES RANGE

As set forth in the Presentence Report, and as stipulated to by the parties, with Tyurin's acceptance of responsibility, the offense level is 36, which with criminal history category of I, yields an applicable advisory Guidelines range of 188 to 235 months' imprisonment. This Guidelines calculation is primarily driven by the grouping of Tyurin's convictions for his involvement in computer hacking, wire fraud, and bank fraud conspiracies, with a base offense level of 7, and the following enhancements:

- a 22-level increase due to a conservative estimate of loss between $25,000,000 and $65,000,000, based on the victim losses from the 1030 offenses, as well as an estimate as to the reasonable foreseeability of the full scope of the conspiracy for the wire and bank fraud conspiracies, *see* U.S.S.G. § 2B1.1(b)(1)(L);

- a 2-level increase because the offense involved 10 or more victims, *see* U.S.S.G. § 2B1.1(b)(2)(A)(i);

- a 2-level increase because a substantial part of the scheme was committed from

outside the United States, the offense involved sophisticated means, and the defendant intentionally engaged in or caused the conduct constituting sophisticated means, *see* U.S.S.G. § 2B1.1(b)(10)(B) and (C);

- a 2-level increase because the offense involved the possession or use of an authentication feature, the unauthorized transfer or use of a means of identification unlawfully to obtain another means of identification, and the possession of five or more means of identification that were unlawfully obtained by the use of another means of identification, *see* U.S.S.G. § 2B1.1(b)(11)(A)(ii) and (C)(i) and (ii);

- a 2-level increase because the defendant was convicted of a § 1030 offense which involved an intent to obtain personal information, *see* U.S.S.G. § 2B1.1(b)(18); and

- a 2-level increase because Tyurin willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice with respect to the investigation, *see* U.S.S.G. § 3C1.1.

(*See* PSR ¶¶ 56-84).

IV. APPLICABLE LAW

Although the Guidelines are no longer mandatory, they continue to play a critical role in trying to achieve the "basic aim" that Congress sought to meet in enacting the Sentencing Reform Act, namely, "ensuring similar sentences for those who have committed similar crimes in similar ways." *United States v. Booker*, 543 U.S. 220, 252 (2005); *see also United States v. Crosby*, 397 F.3d 103, 113 (2d Cir. 2005) ("[I]t is important to bear in mind that *Booker*/*Fanfan* and section 3553(a) do more than render the Guidelines a body of casual advice, to be consulted or overlooked at the whim of a sentencing judge."). "[A] district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range," which "should be the starting point and the initial benchmark." *Gall v. United States*, 552 U.S. 38, 49 (2007). The Guidelines range is thus "the lodestar" that "anchor[s]" the district court's discretion. *Molina-Martinez v. United*

States, 136 S. Ct. 1338, 1345-46 (2016) (quoting *Peugh v. United States*, 133 S. Ct. 2072, 2087 (2013)) (internal quotation marks omitted).

After making the initial Guidelines calculation, a sentencing judge must consider the factors outlined in Title 18, United States Code, Section 3553(a), and "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing: "a) the need to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for that offense; b) the need to afford adequate deterrence to criminal conduct; c) the need to protect the public from further crimes by the defendant; and d) the need for rehabilitation." *United States v. Cavera*, 550 F.3d 180, 188 (2d Cir. 2008) (citing 18 U.S.C. § 3553(a)(2)). Section 3553(a) further directs the Court "in determining the particular sentence to impose" to consider: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the statutory purposes noted above; (3) the kinds of sentences available; (4) the kinds of sentence and the sentencing range as set forth in the Sentencing Guidelines; (5) the Sentencing Guidelines policy statements; (6) the need to avoid unwarranted sentencing disparities; and (7) the need to provide restitution to any victims of the offense. *See* 18 U.S.C. § 3553(a).

In light of *Booker*, the Second Circuit has instructed that district courts should engage in a three-step sentencing procedure. *See Crosby*, 397 F.3d at 103. First, the Court must determine the applicable Sentencing Guidelines range, and in so doing, "the sentencing judge will be entitled to find all of the facts that the Guidelines make relevant to the determination of a Guidelines sentence and all of the facts relevant to the determination of a non-Guidelines sentence." *Id*. at 112; *see also United States v. Corsey,* 723 F.3d 366, 375 (2d Cir. 2013) ("Even in cases where courts depart or impose a non-Guidelines sentence, the Guidelines range sets an important

benchmark against which to measure an appropriate sentence."). Second, the Court must consider whether a departure from that Guidelines range is appropriate. *See Crosby*, 397 F.3d at 112. Third, the Court must consider the Guidelines range, "along with all of the factors listed in section 3553(a)," and determine the sentence to impose. *Id.* at 113. In so doing, it is entirely proper for a judge to take into consideration his or her own sense of what is a fair and just sentence under all the circumstances. *United States v. Jones*, 460 F.3d 191, 195 (2d Cir. 2006).

V. DISCUSSION

Based on the factors set forth in 18 U.S.C. § 3553(a), a sentence within the Guidelines Range is appropriate in this case.

A. The Seriousness of the Offense, and the Need to Promote Respect for the Law and to Provide Just Punishment

The serious nature and circumstances of Tyurin's hacking scheme, as well as the need to promote respect for the law and provide just punishment for the offense, counsel strongly in favor of imposing a Guidelines sentence in this case. *See* 18 U.S.C. § 3553(a)(2)(A). Over the course of approximately eight years, Tyurin worked tirelessly and around the clock on hacking a variety of companies in furtherance of Shalon's criminal enterprise. It was Tyurin's efforts that allowed Shalon to maintain a competitive edge, and allowed Shalon to reap tens of millions of dollars in illicit profits, of which a significant percentage—over $19 million—represented Tyurin's ill-gotten personal gain.[3] Once Shalon and Tyurin turned their attention to companies in the U.S.

[3] To the extent that Tyurin asserts that he only received approximately $5 million in these funds (*see* Mem. at 22), there is no real dispute that Tyurin had considerably more earmarked as his within Shalon's coffers, and that $19 million is a conservative estimate of that amount. Indeed, the communications between the two are replete with regular discussion about how much Shalon owed Tyurin or had transferred to Tyurin and how best to transfer the remainder in a way so as to not arouse suspicion. This included transfers through the use of Russian-based money transfer services commonly used by cybercriminals to launder money, and through the

financial sector, their intrusion activity struck at the heart of the digital operations of major U.S. firms, affording Tyurin and Shalon not only administrator-level access to certain of these firms' networks, but also to the trove of millions of consumers' personal identification information stored therein. A Guidelines sentence is thus necessary in light of the serious nature of the defendant's conduct, as well as the need to promote respect for the law and to provide just punishment. *See* 18 U.S.C. § 3553(a)(2)(A).

Tyurin's characterization of this case as one of "flashy headlines" with "at times near hysterical news coverage," (*see* Mem. at 8) blithely ignores the true harm of Tyurin's hacking activities. To begin, it ignores the considerable resources that were expended by the companies for whom Tyurin's hacking activity was ongoing at the time it was detected. This harm should be seen as distinct from the general Guidelines calculations attendant to crimes under Section 2B1.1, which Tyurin asserts overstates his culpability in this case. (Mem. at 19-22). In recognition of the unique pecuniary harm posed in cases involving a violation of 18 U.S.C. § 1030, the Commentary to Section 2B1.1 contains a special provision regarding loss in the hacking context, which is to be calculated in this context without regard to whether such harm is "reasonably foreseeable" to the defendant:

> Offenses Under 18 U.S.C. § 1030.—In the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.

---

creation of a fictitious contract with invoices to serve as documentary proof to justify wire transfers from Shalon to Tyurin. Thus, the limitation of Tyurin's receipt of funds should properly be viewed not as a mitigating factor, but rather as evidence of additional efforts by the co-conspirators to not draw attention to their criminal activities.

U.S.S.G. § 2B1.1, cmt. n.3(A)(v)(III). Moreover, rather than hold Tyurin responsible for the hundreds of millions of dollars in gambling fraudulent payment processing transactions he played a crucial role in helping facilitate, the Section 2B1.1 loss calculation was based on an extremely conservative estimate of harm, tethered to Tyurin's personal profits (over $19 million) and estimates of loss that were provided to the Government by certain of the victim companies. The restitution sought by the Government representing pecuniary harm to the companies will likely be over $19 million dollars, which represented resources expended by four victim companies in responding to Tyurin's intrusions, pulling employees and resources from their ordinary functions, retaining the services of outside experts, and purchasing hardware necessary to ensure that their vulnerabilities had been patched. This restitution calculation, moreover, is limited to four victims who were identified and/or learned of Tyurin's hacking activities contemporaneously to their being hacked, and as such could readily quantify the harm that was done. Consequently, the restitution amount is an extremely conservative estimate as to actual harm done to the tens of companies harmed by Tyurin over the course of his eight-year partnership with Shalon, both through his hacking and his payment processing fraud.[4]

Tyurin's attempts to distinguish his case from those of other cybercriminals because he did not "steal people's money" or "procure and misuse account numbers, or credit card

[4] With regard to other victim companies hacked by Tyurin, because the evidence of the hacking activity was historical by the time that the Government notified the victims that they had been hacked, in many cases it proved difficult to accurately ascertain the harm that Tyurin's hacking caused. *Cf.* 18 U.S.C. 3663A(c)(3) (allowing court to decline to order mandatory restitution if it finds, from facts on the record, that the number of identifiable victims is so large as to make restitution impracticable, or determining complex issues of fact related to the cause or amount of the victim's losses would complicate or prolong the sentencing process to a degree that the need to provide restitution to any victim is outweighed by the burden on the sentencing process).

information," (Mem. at 8) should be rejected. As the communications between the two reveal, it does not appear that it was Tyurin's moral apprehension about theft of funds that drove his and Shalon's decisions as to how to use the fruits of Tyurin's hacking. Rather, Tyurin was primarily concerned that, if he and Shalon were to actively steal money from individual customers, their criminal activities would more readily be detected by the victim companies. At bottom, Tyurin and Shalon's main concern was how to maximize profit while minimizing the risk of their apprehension. For instance, as part of Tyurin's hacking activities into the U.S. financial firms, Tyurin routinely gained access to passwords not only of network administrators for various firms, but also for individual customers. As a result, in May 2014, Tyurin sought to find investors with the highest deposit balances in their accounts, and subsequently was able to provide Shalon with access into an individual user's trading account at one financial firm [redacted]. Shalon logged into the account, and he sent details to Tyurin about the user's holdings, nothing "What do you think?" "It's simply" "[Expletive] awesome :)" Tyurin, however, warned that "we can get caught" "If two- three people complain, they will start serious investigation" "They will check logins and will change all the passwords." Tyurin also noted that if they did this with accounts that had "recently logged in," it increased the chance that they could "get caught," and thus they should focus instead on "the ones that were [not logging in] for longer than a year." After logging into the account over the course of two days, Shalon and Tyurin lost access to the account. Shalon noted it might have been because their activity had been detected and thus access was blocked, and Tyurin noted "[t]hey have good security." When Tyurin and Shalon speculated on whether they could work together to hack so as to manipulate trading at the victim firm for a short period of time, including, at Tyurin's suggestion, by "break[ing]" the "robots" that helped to execute trades at the company, Shalon suggested that

they find a way to freeze trades for a very short period of time, which would allow them to take advantage of the spread. Tyurin was against this idea not because of any moral qualms, but rather noted "As a whole, I really think that breaking this will expose us," analogizing the risk of being caught as the same as that of breaking into the Pentagon.

In another example, after news reports began to be published regarding the hack of J.P Morgan Chase, Tyurin and Shalon spent many hours speculating as to the progress of law enforcement's investigation, and whether they would be identified as the ones responsible. On October 18, 2014, Tyurin told Shalon "I read how different carders were arrested" "They got everyone through agents" "Like agent gained trust and was buying dumps or cards from them." Shalon responded "Well thank God we don't have anyone" "We don't give anything to anyone" and Tyurin responded "That's true."

As these communications reveal, any limitations in the way in which Tyurin and Shalon sought to monetize the fruits of Tyurin's hacking crimes were fundamentally driven by pragmatic considerations regarding the risk of their detection and ultimately their apprehension, rather than concerns regarding relative moral culpability of their use of the stolen data. Put another way, because Shalon's and Tyurin's means to profit from their criminal behavior were more akin to a sophisticated business enterprise, they did not have to resort to the riskier tactics of monetizing the stolen data on the black market or "sluic[ing] funds out of people's accounts." (*See* Mem. at 8). Moreover, and importantly, once Tyurin rendered these networks vulnerable and stole the customer data for Shalon, his conduct left those millions of individuals vulnerable to further crimes, lest that data get into the hands of others. In this regard, Tyurin's attempts to minimize the harm that resulted to individual customers by taking the position that there is no evidence that any identity theft or related fraud occurred to the customers, and that one of the companies

declined to provide credit monitoring to their customers. (Mem. at 10-11 & n.1). This is of little comfort to those customers of the financial institutions and brokerage firms who, when faced with the anxiety about their identity being stolen and the security of their finances, elected to enroll in credit monitoring services and other efforts to secure their online identities as a result of being notified of the breach.

In addition, although Tyurin now attempts to draw a distinction between his relative moral culpability and those who engage in credit card theft, communications between him and Shalon from before their arrests tell a different story regarding Tyurin's views regarding the comparability of these types of crimes. For instance, after news reports of the investigation into the J.P. Morgan Chase hack continued, in March 2015, Tyurin and Shalon discussed the likelihood that Shalon would be arrested and extradited from Israel to the United States, and whether he would be charged just with the hacking or also with the online gambling offenses. In an effort to weigh the benefits of Shalon fleeing to another country, Tyurin referenced the case of Vadim Vassilenko, whom he described as "the one who did Western Express and helped with money laundering [who] was imprisoned for eight years in USA." Vassilenko's case was an investigation and prosecution by the United States Secret Service and the Manhattan District Attorney's office into the Western Express Cybercrime Group, which press reports noted was responsible for approximately $5 million in credit card theft.[5] This conversation suggests that Tyurin himself believed at the time that illegal carding activities were comparable to his own

[5] *See, e.g.,* Wired Magazine, "5 More Indicted in Probe of International Carding Ring," Sept. 1, 2009 (*available at* https://www.wired.com/2009/09/westernexpress/); Wired Magazine, "Ukrainian Carder in $5 Million Ring Sentenced to 14-Plus Years in Prison," Aug. 9, 2013 (*available at* https://www.wired.com/2013/08/carder-eskalibur-sentenced/).

crimes when evaluating the consequences that he and Shalon might face if they were apprehended.

Finally, it is worth noting that, contrary to Tyurin's description, his role was not simply to follow Shalon's orders or "procur[ing] lists of potential targets for electronic marketing," without regard as to "what was eventually done with the lists." (*Contra* Mem. at 22). Rather, the communications between Shalon and Tyurin paint a different picture, where the two were criminal partners, each possessing unique skills and focusing on executing different aspects of their crimes, but where each partner had significant input as to their mutual endeavors. The communications show that Tyurin and Shalon brainstormed together various ways in which the stolen data could be monetized, and decisions as to whether or not to pursue these various options were made after carefully balancing their potential profits against the risks of getting caught, with input from both partners. In one instance, Tyurin sought to convince Shalon to "break into *Goldman Sachs*, they know everything." In another, Tyurin pushed back on Shalon's view to simply download all the data at J.P. Morgan Chase blindly, but rather instead to focus on specific types of data. Tyurin first suggested identifying the investors, because "[t]here is probably [a] shitload of information on various shenanigans that they are doing," and that they should be focused on identifying the "VIP clients" and downloading their data, including their balances. Tyurin then suggested on trying to identify the best investment managers at J.P. Morgan Chase and analyze what they were doing, noting that "JPM is 15% of USA GDP" "Their capital." These communications show that Tyurin was not a simple employee of Shalon's who was following orders; rather, because Tyurin possessed the technical skills upon which Shalon's entire criminal enterprise depended, Tyurin and Shalon worked together as partners, making mutual

decisions about what steps to take with regard to executing the hacks, brainstorming what type of data would be most useful to take, and deciding what to do with the data once it was stolen.

For all these reasons, Tyurin's arguments as to his relative lesser moral culpability as compared to other hacking defendants are without merit. To the extent that Tyurin "could not bring himself" to steal money directly from individual customers of these banks, his own statements strongly suggest this was not out of any concern for any of the victims of his criminal activities. (*Contra* Mem. at 11). Rather, it was simply because Tyurin was most concerned about needlessly increasing the risk that he and Shalon would be caught, and the consequences to their profitable criminal enterprise that would follow.

B. The Need to Avoid Unwarranted Sentence Disparities Among Similar Defendants

A Guidelines sentence such as that sought by the Government would also comport with "the need to avoid unwarranted sentence disparities among defendants." 18 U.S.C. § 3553(a)(6); *see also United States v. Ghailani*, 733 F.3d 29, 55 (2d Cir. 2013). As described above, Tyurin's criminal conduct was wide ranging and targeted a variety of industries in order to further numerous different types of criminal activity, including securities fraud, illegal gambling, and payment processing fraud. Thus, when compared against sentences for defendants convicted of hacking offenses of equivalent breadth, scope, and duration, a Guidelines sentence for Tyurin ensures that there are no unwanted sentencing disparities between Tyurin and other similarly culpable defendants. In this District and elsewhere, the sentences for sophisticated hackers meted by judges have been significant and lengthy. For instance, in *United States v. Jeremy Hammond*, No. 12 Cr. 185 (LAP), the defendant was a recidivist computer "hacktivist" who between 2011 and 2012 hacked numerous businesses, individuals, and local law enforcement-

related entities in order to deface websites and steal and post personal data, resulting in losses between $1 million and $2.5 million. The advisory Guidelines range for the defendant was the statutory maximum of 120 months' imprisonment; but for that statutory cap, the range would otherwise be 151 to 188 months *See id.*, Gov't Sentencing Mem., Dkt. No. 60 (Nov. 12, 2013). Judge Preska sentenced the defendant to 120 months. More recently, in *United States v. Hamza Bendelladj*, No. 11-CR-557-AT-2, in the Northern District of Georgia (the District from which certain of the counts to which Tyurin pleaded guilty originated), the defendant, an Algerian-national hacker who managed botnets and used them to steal bank and credit card information belonging to 200,000 people, was arrested in Thailand while he was in transit from Malaysia to Algeria, extradited to the United States, and subsequently pleaded guilty to 23 felony counts. *See id.*, Gov't Sentencing Mem., Dkt. No. 158 (Mar. 2, 2016). Ultimately, Bendelladj's offense level was calculated as 34, yielding an Guidelines range of 151 to 188 months' imprisonment, and he was sentenced to 143 months' imprisonment. *See id.*, Dkt. No. 242, at 5 n.4 (Nov. 20, 2019) (adjusted Guidelines calculation in light of incorrect application of § 2B1.1(b)(4) enhancement); Amended Judgment, Dkt. No. 254 (Mar. 24, 2020). Finally, in *United States v. Yevgeniy Nikulin*, No. 16 Cr. 440 (WHA), in the Northern District of California, the defendant, a Russian national, was found guilty after trial of hacking into LinkedIn, Dropbox, and a social networking company known as Formspring. The evidence at trial established that the defendant installed malware on their networks, stole and then used login credentials for employees, and subsequently conspired to sell customer data stolen from these networks. It is the Government's understanding that the advisory Guidelines range was 108 to 131 months' imprisonment, with a consecutive 24 month term; the Judge sentenced Nikulin principally to 88 months' imprisonment, and noted in his pronouncement his consideration of general deterrence attendant to the sentence, and his hope

that the sentence would send a clear message to deter anyone, including persons abroad, from engaging in similar conduct. *See id.*, Gov't Sentencing Mem., Dkt. No. 277 (Sept. 22, 2020); Judgment, Dkt. No. 281 (Oct. 5, 2020); Press Release, "Russian Hacker Sentenced to Over 7 Years in Prison for Hacking into Three Bay Area Tech Companies."[6]

Indeed, if evaluated by the metric of the number of victim companies that were hacked, and the harm done to those victim companies, Tyurin's crime should properly be seen as analogous to cases which resulted in significant incarceratory sentences, which he seeks to distinguish in his memorandum. For instance, in *United States v. Drinkman*, No. 09 Cr. 626 (JBS) (D. N.J.) (cited at Mem. at 11 n.2), Vladimir Drinkman, a Russian national who was extradited from the Netherlands, had hacked into 17 companies, including payment processors and financial institutions comparable to those hacked by Tyurin. It is the Government's understanding that Drinkman had an offense level of 38 (235 to 293 months' imprisonment), which is higher than that of Tyurin because it was driven by the volume of fraudulent credit card transactions. Drinkman was sentenced to 144 months' imprisonment. *See id.*, Plea Agreement, Dkt. No. 82 (Sept. 15, 2015); Minute Entry, Dkt. No. 116 (Feb. 14, 2018). And in *United States v. Findikoglu*, No. 13 Cr. 440 (KAM) (E.D.N.Y.) (cited at Mem. at 11 n.2), Ercan Findikoglu, a Turkish national, was convicted of having hacked into three companies between 2011 and 2013, a comparably more limited period and scope of criminal activity than that of Tyurin. In light of the loss amount calculated at $55 million, again driven by fraudulent transactions, the Guidelines range for Findikoglu was 135 to 168 months' imprisonment; Findikoglu was sentenced to 96

[6] *Available at* https://www.justice.gov/usao-ndca/pr/russian-hacker-sentenced-over-7-years-prison-hacking-three-bay-area-tech-companies.

months' imprisonment by Judge Matsumoto. *See id.*, Gov't Sentencing Mem., Dkt. No. 35 (Jan. 31, 2017); Judgment, Dkt. No. 39 (Feb. 16, 2017).

It is also worth noting that Tyurin's participation in the online gambling schemes—which Tyurin understood were among the most lucrative for Shalon's enterprise—did not have a material effect on the Guidelines calculation as compared to his grouped counts of conviction under § 2B1.1. In part, this is because the Guidelines calculation for gambling offenses is governed by U.S.S.G. § 2E3.1. As applied in Tyurin's case, the Guidelines calculation for his gambling offenses had a relatively low and capped adjusted offense level of 12, reflective of the structure of § 2E3.1, and thus were disregarded for purposes of the Guidelines in light of their being more than 9 levels less serious than the level for the grouped offenses under § 2B1.1. *See* U.S.S.G. § 3D1.4(c). Nevertheless, as the Guidelines suggest, the online gambling offenses "may provide a reason for sentencing at a higher end of the sentencing range for the applicable offense level." U.S.S.G. § 3D1.4(c).

Relatedly, with regard to the relatively limited incarceratory sentences for defendants in gambling cases upon which Tyurin relies (Mem. at 13-14), it is worth noting that these defendants had significantly lower applicable advisory Guidelines ranges because of the application of § 2E3.1, but nevertheless received above-Guidelines sentences. For instance, in *United States v. Tzvetkoff*, No. 10 Cr. 336 (LAK), defendant Ira Rubin, a payment processor, pleaded guilty to three counts (Unlawful Internet Gambling Enforcement Act conspiracy; conspiracy to commit bank and wire fraud; and money laundering conspiracy) and had an applicable Guidelines range of 18 to 24 months' imprisonment (much less than that of Tyurin). *See id.*, S3 Indictment, Dkt. No. 20 (Apr. 14, 2011); Gov't Sentencing Mem., Dkt. No. 212 (July 24, 2012). Nevertheless, Judge Kaplan sentenced Rubin to an above-Guidelines sentence of a three-year term of

imprisonment. *See id.*, Judgment, Dkt. No. 223 (Aug. 6, 2012). Similarly, in *United States v. Tokhtakhounov, et al.*, 13 Cr. 268 (JMF), defendant Anatoly Golubchik pleaded guilty to one count of participation in a racketeering conspiracy, and had a Guidelines range of 21 to 27 months' imprisonment. Judge Furman sentenced Golubchik to an above-Guidelines sentence of 60 months' imprisonment. *See id.*, Gov't Sentencing Mem. at 10, Dkt. No. 866 (Apr. 22, 2014); Judgment, Dkt. No. 894 (Apr. 29, 2014).

For payment processing, it is worth using as a benchmark the sentences in the related prosecution of *United States v. Anthony Murgio*, No. 15 Cr. 769 (AJN), in which the Government brought charges against the U.S.-based co-conspirators who ran the unlicensed illicit bitcoin exchange Coin.mx, owned by Shalon. As described above, Coin.mx relied on Shalon's fraudulent payment processing system in order to run its bitcoin transactions, and as such, the Guidelines range for the lead defendant, Anthony Murgio, was driven by the volume of bitcoin transactions in light of his convictions for bank and wire fraud. Coin.mx, however, represents but a small fraction of the volume of Shalon's criminal payment processing schemes. And in contrast to Anthony Murgio, whose work was solely related to Coin.mx, Tyurin's role was crucial to every facet of Shalon's criminal conglomerate, including the entirety of his payment processing operation. Thus, Anthony Murgio's 66-month sentence from Judge Nathan should be viewed as a sentence of a defendant much less culpable than Tyurin.

Finally, with regard to Tyurin's hacking of the U.S. financial sector companies in furtherance of Shalon's securities fraud scheme, Tyurin points to the "relatively modest" gains to the defendants as a result of the securities fraud scheme as a way to minimize the seriousness of these counts of conviction. (*See* Mem. at 9). But, as is described above, because the harm here should best be framed as the harm Tyurin's hacking imposed upon the victim companies, as

evidenced by the significant requests for restitution, Tyurin's argument regarding the relative lack of harm from his hacking of major financial companies in furtherance of securities fraud should be rejected. Moreover, even in analogous cases involving hacking linked to securities fraud, Tyurin's case stands apart in terms of size, scope, and impact. For instance, in *United States v. Christopher Rad*, No. 11 Cr. 161 (JAP) (D. N.J.), the defendant was convicted after trial for using hackers to illegally spam victims in furtherance of a securities pump-and-dump scheme over the course of approximately 16 months; Rad, who was the central organizer of the scheme, made approximately $2.8 million as a result, and paid the hackers more than $1.4 million. Despite this, Judge Pisano sentenced Rad principally to 71 months' imprisonment, a significant incarceratory sentence. *See id.*, Opinion, Dkt. No. 93 (Jan. 16, 2013); Press Release, "Organizer of International Securities Fraud Ring Sentenced to Prison for Using Hackers to Falsely Inflate Stock Prices."[7]

In sum, the cases in this District and elsewhere, the significant incarceratory sentences that have been issued for defendants similarly situated to Tyurin strongly counsel in favor of a significant Guidelines period of incarceration in this case.

C. The Need to Afford Adequate Deterrence

The sentence sought by the Government is also necessary here to "afford adequate deterrence to criminal conduct." 18 U.S.C. § 3553(a)(2)(B). The public's interest in deterrence is particularly acute in cases like this, because deterrence is essential to reducing the ever-increasing costs of computer hacking.

[7] *Available at* https://archives.fbi.gov/archives/newark/press-releases/2013/organizer-of-international-securities-fraud-ring-sentenced-to-prison-for-using-hackers-to-falsely-inflate-stock-prices.

As was true in this investigation, investigations of major hacking cases are challenging, as investigators and law enforcement must work quickly to collect and preserve data from around the world before the bad actors have destroyed or encrypted it, analyze that data to accurately attribute the work to a particular individual, and then successfully apprehend that individual, oftentimes relying on extradition requests of foreign countries. Indeed, even in instances where U.S. law enforcement successfully collects the requisite evidence and identifies the actors at issue, bringing those individuals to justice in a U.S. court poses its own challenges, and the Government publicly announces charges without apprehending the defendants. *See, e.g., United States v. Rafatnejad et al.*, 18 Cr. 94 (JMF) (charges announced against nine Iranian nationals who conducted cyber theft campaign against universities and companies to steal research, academic and proprietary data); *United States v. Hua et al.*, 18 Cr. 891 (VSB) (charges announced against two Chinese hackers who targeted intellectual property and confidential business information); *United States v. Iat Hong et al.*, 16 Cr. 360 (SHS) (charges announced against four individuals for insider trading based on information hacked from U.S. law firms; extradition request for defendant arrested in Macau was denied). Of note, this category includes charges in two cases which were publicly announced against foreign hackers responsible for stealing data used in securities fraud schemes; in both cases, the hackers remain at large. *See, e.g., United States v. Ivan Turchynov*, No. 15 Cr. 390 (D. N.J.) (charges against Ukrainian hacker and co-conspirators for stealing confidential information about publicly traded companies from newswire victim companies); *United States v. Artem Radchenko*, No. 19 Cr. 30 (D. N.J.) (charges against Ukrainian national for hacking into Securities and Exchange Commission's EDGAR system and stealing confidential, non-public financial information about publicly traded companies). The *Turchnyov* case was of particular interest to Tyurin, because he had previously been approached

to join that conspiracy. Tyurin sent a Shalon a link to a Russian-language article which described the charges had been brought, and that while the U.S.-based traders had been arrested, the Ukrainian hackers had not:

```
Tyurin:    By the way, do you remember those Prnewswire and
           Business wire?
Tyurin:    I told about them
Tyurin:    Something like dudes who wanted to do shady stuff
           with press releases.
Shalon:    You said something like that when we met each
           other.
Shalon:    [question mark]
Tyurin:    Yes.
Tyurin:    In a year or two since we met.
Shalon:    At the exchange, right?
Tyurin:    Yes.
Shalon:    Yes.
Shalon:    I remember it now.
Tyurin:    Those dudes were caught.
Tyurin:    http://inosmi.ru/world/20150812/229589716.html
Tyurin:    From Ukraine.
```

As a result of the significant resources required to mount a successful hacking prosecution, convictions are relatively rare. Consequently, the importance of affording general deterrence through meaningful sentences is particularly acute in criminal hacking cases: where the incidence of prosecution is lower, the level of punishment must be higher to obtain the same level of deterrence. Moreover, the need for general deterrence is greatest in cases involving particularly lucrative and difficult-to-detect hacking schemes, such as the sophisticated schemes in which Tyurin and Shalon participated. In light of the significant public interest in this case, including its coverage in the press, the sentence that Tyurin will send a message to others here and elsewhere about the consequences that may befall them if they engage in similar behavior.

The particular need for general deterrence in hacking cases such as Tyurin's has previously been recognized by Judges in this District. For instance, in *United States v. Knowles*,

16 Cr. 5 (PAE), the defendant pleaded guilty to having hacked into email accounts of victims in the entertainment, sports, and media industries, and stolen scripts of movies and television shows that had yet not yet aired, as well as personally identifiable information of the victims. After determining that the appropriate Guidelines range was 27 to 33 months' imprisonment (a range significantly lower than that of Tyurin), Judge Engelmayer sentenced the defendant principally to an above-Guidelines sentence of 60 months' imprisonment. In imposing this sentence, Judge Engelmayer aptly articulated the importance of general deterrence as follows:

> At a time when much of the world has a presence on the Internet, at a time when so many people in this country and abroad keep sensitive material on line, whether personal data or confidential business information or works, at a time when remote hacking is regrettably an all-too-common topic in our news, it is vitally important that the law muscularly respond to the modern-day pirates like you who would plunder that material.
>
> The sentences in such cases of cybercrime need together to send a message that significant punishment awaits hackers who access accounts for purposes of theft and self enrichment. The sentence imposed here has the potential to convey that message to those, Mr. Knowles, who would follow your lead.
>
> That message is particularly acute in the context of international hackers. You carried your scheme from the Bahamas. Only the creative sting arranged by the undercover lured you to the United States where you were arrested. But for hackers who operate for abroad who damage the lives and business interests of Americans by remote means, it will often be hard to law enforcement to catch up with them.
>
> It's an unfortunate reality, but between different legal regimes, limited across-border cooperation among law enforcement, and the inherent challenges of identifying and catching cyberthieves, the difficulty of apprehending an overseas hacker is reality. So it is all the more important that when a hacker from outside the United States is caught, the punishment be meaningful to convey to others who operate from afar, so that even if the likelihood of apprehension may not be great, the consequences will be.
>
> I judge the interest in general deterrence as substantial.

See United States v. Knowles, Sentencing Tr. 49-51 (Dec. 6, 2016). It is without question that Tyurin's criminal activity, in contrast to that of Knowles, is greater in magnitude, scale, and duration, and thus the punishment here should be commensurately greater than that of Knowles.

The public's interest in deterring cybercrime cannot be overstated. According to one estimate, the average total cost in 2017 to a victim company from a data breach was approximately $7.35 million. *See* Report of the Attorney General's Cyber Digital Task Force, July 2, 2018, at 27.[8] The Internet Crime Complaint Center ("IC3"), the FBI unit that receives and tracks cybercrime complaints from victims, received a total of 1,795 complaints of corporate data breach in 2019, with reported losses exceeding $53 million. *See* Federal Bureau of Investigation, 2019 Internet Crime Report, at 20.[9] These figures are no doubt reflective of the fact that compromises to a company's systems impose a tremendous cost, because the victim company must expend considerable resources to identify the full scope of the breach and fix any vulnerabilities, ensure the protection of PII and other sensitive data, notify their customers, and report and respond to federal and state regulatory agencies in the aftermath of a breach.

Criminals such as Tyurin use increasingly sophisticated tools and techniques to obfuscate their true identities and their infrastructure is frequently scattered across multiple international jurisdictions, as was the case here. With minimal capital investment, Tyurin was able to profit richly from his criminal activity by stealing data from protected computer networks in the United States and elsewhere, all while safely sitting in front of his computer half a world away. Identifying hackers such as Tyurin and bringing them to justice requires a substantial commitment

[8] *Available at* https://www.justice.gov/ag/page/file/1076696/download (citing Ponemon Institute, 2017 Cost of Data Breach Study: United States, at 1).
[9] *Available at* https://pdf.ic3.gov/2019_IC3Report.pdf.

of law enforcement resources. In light of the success of law enforcement in dismantling this criminal organization, it is imperative to deter other potential cybercriminals by sending a clear message that they risk severe consequences if they choose to attack U.S. companies and steal the personal information of U.S. customers. *Cf. United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994) ("Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it.").

For all these reasons, it is clear that sentences for multi-year criminal hacking schemes, where hackers such as Tyurin engage in the conduct against U.S. victims from the comfort of their homes thousands of miles away, should be substantial, in order to afford adequate deterrence.

VI. CONCLUSION

The facts of this case warrant a serious penalty. Tyurin used his unique skills over an extended period of time to hack and victimize over a dozen companies and steal consumer data for over 100 million U.S. customers. And when it became apparent that his actions were being investigated by authorities, he and his co-defendant worked together to destroy evidence of his crimes, and to obstruct U.S. law enforcement in their efforts to identify them.

The Government respectfully submits that, based on the facts and arguments set forth above, a significant Guidelines sentence is appropriate in this case.

Dated: New York, New York
November 12, 2020

Respectfully submitted,

AUDREY STRAUSS
Acting United States Attorney
Southern District of New York

By: /s/
Eun Young Choi
Assistant United States Attorney

cc: Florian Miedel, Esq. (by email)